Table 3: A summary for applying deep learning (DL) techniques to the SDN paradigm

Reference	DL Approach	Task	Findings
Tang et al. [44]	GRU-RNN	Intrusion detection	Outperformed DNN [149], SVM and NB Tree with an accuracy of 89%.
Mao et al. [55]	DBN	Routing	Outperformed OSPF protocol in terms of throughout and average delay per hope.
Zhang et al. [56]	SAE	Feature extraction for network application classification	Outperformed SVM in terms of accuracy, precision, recall and F1-measure.
Niyaz et al. [57]	SAE	Feature extraction for DDoS detection	An accuracy of 95.65%, 99.82% for 8-class and 2-class classification respectively. Outperformed soft-max and neural network classifiers.
Liu et al. [58]	SAE	Feature extraction for content popularity prediction in information centric network	Accuracy improvements over neural networks and auto regressive, 2.1%-15% and 5.2%-40% respectively.
Tang et al. [149]	DNN	Intrusion detection	Outperformed Naive Bayes, SVM and DT with an accuracy of 75.75%.
Lazaris and Prasanna [150]	LSTM-RNN	Time series traffic prediction	An average mean absolute percentage error (MAPE) of 12% for approximating real flow sizes on CAIDA traces and MAPE of 3.9% on simulating the network topology of Google's B4.
Azzouni and Pujolle [151]	LSTM-RNN	Traffic matrix prediction	Outperformed an efficient dynamic routing heuristic by finding the near optimal path in shorter time using generated data.
Azzouni and Pujolle [152]	LSTM-RNN	Traffic matrix prediction	Outperformed linear forecasting models (ARMA, ARAR, HW) and feed forward neural network (FFNN) using real data.
Huang et al. [153]	Deep MLP (DNN), CNN and LSTM	Adversarial attacks on SDN-based deep IDS	JSMA attack showed a significant impact on the deep ML models ranges from 14 to 42%, JSMA-RE reduced the accuracy of MLP to 35%. FGSM caused a significant reduction in the accuracy of LSTM (more than 50%).
Stampa et al. [179]	Deep deterministic policy gradients	Routing	Outperformed their primary benchmark.
Streiffer et al. [181]	A3C	Automating data center network topologies management	Finds near optimal solutions across a range of topologies.

5.1.4 Semi-supervised learning in SDN

Semi-supervised learning [182-185] were also used in SDN, but much less common compared with other learning approaches. The research was focused on traffic classification [182, 184], routing [183] and intrusion detection [184]. Wang et al. [182] proposed a new framework for QoS-aware traffic classification based on semi-supervised learning. This approach can classify the network traffic according to the QoS requirements. The system allows achieving deep packet inspection (DPI) and semi-supervised learning based on Laplacian SVM. The Laplacian SVM approach outperformed a previous semi-supervised approach based on k-means classifier.

Chen and Zheng [183] introduced an efficient routing predesign solution based on semi-supervised approach. The study suggested using an appropriate clustering algorithm such as Gaussian mixture model and k-means clustering for feature extraction. Thereafter, a supervised classification approach such as extreme learning machine (ELM) can be used for flow demand forecasting. The authors also suggested using an adaptive multipath routing approach based on analytic hierarchy process (AHP) for handling to elephant flows according different constraint factor weights.

Li et al. [184] proposed a new method for fine-grained traffic classification based on semi-supervised approach called nearest application based cluster classifier (NACC). Unlike traditional methods, which use one feature vectors, this algorithm constructs a matrix with several cluster centroids based on k-means clustering to represent the application. The algorithm uses a small number of labelled flows to build a supervised dataset. Then collects the unlabelled flows to be merged with previously collected dataset, based on investigating the correlated flows, which is used to map an application to different clusters. The experimental results showed a good identification accuracy reaching 90%.

Wang et al. [185] introduced an intrusion detection method based on semi-supervised approach for wireless SDN-based e-health monitoring systems. The proposed system employed the concept of off-line training and on-line testing to allow running localized intrusion detection on wireless massive machine-type communications (mMTC) devices. Their system adopts semi-supervised learning on the basis of modified contrastive pessimistic likelihood estimation (CPLE), in which they replace the maximization calculation by a relaxation function. CPLE [186] performs semi-supervised parameter estimation for likelihood-based classifiers. The proposed modified CPLE outperformed Naive Bayes, SVM, DNN, self-training (semi-supervised approach) and the original CPLE based on the experiments conducted on NSL-KDD dataset.

5.2 Meta-heuristic Algorithms Used in SDN

A large variety of meta-heuristic algorithms such as ant colony optimization [187-195], evolutionary algorithms [196-198], genetic algorithms [199-207], particle swarm optimization [208-213], simulated annealing [214-216], bee colony optimization-based [217,218], whale optimization [219,220], firefly optimization [221], bat algorithm [88], teaching-learning-based optimization [90] and grey wolf optimization [222] were used in SDN.

5.2.1 Ant colony optimization in SDN

ACO has been widely used for solving various networking problems such as routing [187-189,192], load balancing [190,191], network security [193,194] and maximizing net-